COMMENTS

AN UNBALANCED STANDARD: SEARCH AND SEIZURE OF ELECTRONIC DATA UNDER THE BORDER SEARCH DOCTRINE

Rachel Flipse[*]

The evolution of technology frequently leads to conflict between the protection of civil liberties and the government's need to preserve national security.[1] As the world becomes dangerous in new ways, new techniques are developed to combat the hazards. This can have the unfortunate side effect of eroding individual protections until the laws that ensure them evolve to catch up. This tension is exemplified by the application of the border search exception to the Fourth Amendment, which allows for warrantless and suspicionless searches of the luggage of anyone crossing the United States border,[2] to data stored on laptop computers and other electronic devices such as cell phones and personal digital assistants.

It may surprise many travelers to learn that any time they enter or leave the United States, the Department of Homeland Security claims

---

* J.D. Candidate, 2010, University of Pennsylvania Law School; B.A. Psychology 2007, The George Washington University. I would particularly like to thank Professors David Rudovsky and Theodore Ruger for their insightful suggestions. I would also like to thank my Comment Editor, Aamir Wyne, for his assistance during the writing process and the staff of the *Journal of Constitutional Law* for all of their hard work.

1 *See* Jerel A. Rosati, *At Odds with One Another: The Tension Between Civil Liberties and National Security in Twentieth-Century America*, *in* AMERICAN NATIONAL SECURITY AND CIVIL LIBERTIES IN AN ERA OF TERRORISM 9, 9 (David B. Cohen & John W. Wells eds., 2004) ("The demands of democracy and the demands of national security inherently have contradictory implications . . . ."); *see also* Kyllo v. United States, 533 U.S. 27, 34 (2001) (discussing the potential impact of new technologies on "the realm of guaranteed privacy" as a matter that the Supreme Court must confront). *See generally* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004) (arguing that courts should approach the Fourth Amendment with caution when technology is in flux).

2 *See* United States v. Ross, 456 U.S. 798, 823 (1982) (noting that Customs officers have the authority to search luggage entering the United States at random in the absence of individualized suspicion); United States v. Ramsey, 431 U.S. 606, 616 (1977) (stating that typically, border searches "are reasonable simply by virtue of the fact that they occur at the border"). The exception to the warrant requirement applies to searches taking place at the physical border as well as international airports within the United States, considered to be the "functional equivalent[]." Almeida-Sanchez v. United States, 413 U.S. 266, 273 (1973).

the right to search, seize, and duplicate the information contained in their laptops, BlackBerrys, and other electronic storage devices.[3] Although the Supreme Court has not yet spoken on this issue, a few travelers have challenged the constitutionality of such searches, and the matter has been addressed by several circuit courts. Most recently, in April 2008, the Ninth Circuit reversed the District Court's holding[4] in *United States v. Arnold* and accepted the government's contention[5] that Customs officers and Department of Homeland Security agents may search, seize, and even copy information contained in electronic devices without cause or suspicion.[6]

This Comment analyzes the ambiguities and potential constitutional problems posed by this practice. They continue to be a threat, despite some improvements in the protection of civil liberties implemented by the Obama administration. The Comment discusses the failure of the lower federal courts to adequately balance the privacy and confidentiality concerns of the law-abiding traveler against potential but unlikely national security threats, and the resulting weakening of the traditional protections afforded by the Fourth Amendment. It concludes by suggesting stronger protective measures in several areas, as well as avenues of recourse for the traveler facing such a search. The adoption and implementation of these could go a long way toward striking a more appropriate balance between national security and the constitutional guarantee of individual freedom from unreasonable search and seizure.

---

3 *See, e.g.*, Nathan Alexander Sales, *Run For the Border: Laptop Searches and the Fourth Amendment*, 43 U. RICH. L. REV. 1091, 1092 (2009) ("When told that the government claims the power to rummage through travelers' laptops, BlackBerrys, and flash drives at the border, many people react with shock, even revulsion."); Press Release, Ass'n of Corporate Travel Executives, ACTE Survey Shows Threat of Laptop Seizure at U.S. Borders Still Unknown to International Business Travelers (Jan. 31, 2008), *available at* http://www.acte.org/resources/press_release.php?id=267 (announcing results of a survey by the Association of Corporate Travel Executives showing "that a huge segment of [individuals] responsible for the international transportation assets of companies . . . indicated they were unaware that computers and other devices, such as Blackberrys, iPhones, iPods, flashdrives and cameras, can be examined, searched, and seized—without warrant nor provocation—when crossing a U.S. border").

4 United States v. Arnold, 454 F. Supp. 2d 999 (C.D. Cal. 2006), *rev'd*, 523 F.3d 941 (9th Cir. 2008).

5 Government's Opening Brief at 17, United States v. Arnold, 523 F.3d 941 (9th Cir. 2008) (No. 06-50581).

6 *See Arnold*, 523 F.3d at 946.

I. HISTORY OF THE BORDER SEARCH DOCTRINE

The Fourth Amendment of the United States Constitution states, in relevant part, that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation."[7] When a governmental search or seizure will violate an individual's reasonable expectation of privacy, the searcher is typically required to obtain a warrant in advance.[8] Warrants ensure that an impartial magistrate has reviewed the circumstances and found sufficient probable cause of wrongdoing to justify a search and the resulting invasion of privacy.[9]

Congress[10] and the Supreme Court[11] have definitively established the existence (though not the precise parameters) of recognized exceptions to the warrant requirement in certain situations,[12] including the border search doctrine. In 1985, the Court held in *United States v. Montoya de Hernandez* that warrants were not required for "routine" border searches, and that such searches could be performed in the absence of probable cause or even reasonable suspicion.[13] Examination of luggage is almost unquestionably necessary so that Customs agents can ensure that narcotics, explosives, and the like are not entering the country. Even those who oppose the application of the border search doctrine to computers and electronic devices agree

---

7 U.S. CONST. amend. IV.

8 U.S. DEP'T OF JUSTICE, EXECUTIVE OFFICE FOR UNITED STATES ATTORNEYS, OFFICE OF LEGAL EDUCATION, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 2–3 (2001).

9 *See* McDonald v. United States, 335 U.S. 451, 455 (1948) ("[T]he Fourth Amendment has interposed a magistrate between the citizen and the police . . . so that an objective mind might weigh the need to invade that privacy in order to enforce the law.").

10 *See* 19 U.S.C. § 1581(a) (2006) ("Any officer . . . may at any time go on board of any vessel or vehicle at any place in the United States . . . [search the vehicle] . . . and any person, trunk, package, or cargo on board . . . ."). Federal courts have warned that this statute must be read "in light of the [F]ourth [A]mendment's requirement that searches and seizures be reasonable." Blair v. United States, 665 F.2d 500, 505 (4th Cir. 1981).

11 *See* United States v. Ramsey, 431 U.S. 606, 619 (1977) ("[The] longstanding recognition that searches at our borders without probable cause and without a warrant are nonetheless 'reasonable' has a history as old as the Fourth Amendment itself.").

12 Other exceptions to the warrant requirement include the plain view doctrine, discussed in *Texas v. Brown*, 460 U.S. 730 (1983), searches made incident to a lawful arrest, addressed in *Chimel v. California*, 395 U.S. 752 (1969), and searches made under exigent circumstances, explained in *United States v. Smith*, 797 F.2d 836 (10th Cir. 1986).

13 473 U.S. 531, 541 (1985).

that Customs agents must have the ability to search the belongings and person of travelers for contraband and other dangerous items.[14]

Even at the border, where the federal government's national security authority receives enormous deference, search authority is not unlimited. The Supreme Court has held that "interests in human dignity and privacy which the Fourth Amendment protects" require that a standard of reasonable suspicion be met before invasive body searches are permissible.[15] Lower courts have interpreted this to mean that, at least when applied to searches of the body, "[a]s the search becomes more intrusive, more suspicion is needed."[16]

The United States Supreme Court has also left open the possibility that searches of property could be so offensive, intrusive, or destructive as to require a finding of particularized suspicion or probable cause to render them constitutional.[17]

One helpful, although somewhat imprecise, way of conceptualizing the historical approach to search and seizure at the United States border is to divide searches into two categories: "routine" and "non-routine."[18] "Routine" searches, such as the typical examination of the contents of an individual's luggage or pockets, do not require any suspicion.[19] "Non-routine" searches, while not limited by the "probable cause" and warrant requirements[20] present within the United

---

14 *See, e.g.*, Nanci Clarence & Craig Bessenger, *They Have Ways of Making Your Laptop Talk*, THE RECORDER, July 2, 2008, *available at* http://www.law.com/jsp/PubArticle.jsp?id=1202422588869 (criticizing the Ninth Circuit's "cursory analysis of computers in the Fourth Amendment context," but acknowledging that "border searches date from the nation's earliest years, and the United States has a clear interest in intercepting contraband at the border").

15 *Montoya de Hernandez*, 473 U.S. at 540 (1985) (citing Schmerber v. California, 384 U.S. 757, 769–70 (1966)). *Montoya de Hernandez* defines "reasonable suspicion" by analogizing to the following language from *Terry v. Ohio*, 392 U.S. 1, 21 (1968): "[I]n justifying the particular intrusion the police officer must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion." *Id.* at 540.

16 United States v. Vance, 62 F.3d 1152, 1156 (9th Cir. 1995).

17 *See Montoya de Hernandez*, 473 U.S. at 541–42 (noting that border officials must have a "'particularized and objective basis for suspecting the particular person' of alimentary canal smuggling" before performing an alimentary canal search); United States v. Ramsey, 431 U.S. 606, 618, n.13 (1977) ("[A] border search might be deemed 'unreasonable' because of the particularly offensive manner in which it is carried out."); United States v. Arnold, 523 F.3d 941, 945 (9th Cir. 2008) ("[T]he Supreme Court has held open the possibility, 'that some searches of *property* are so destructive as to require' particularized suspicion." (quoting United States v. Flores-Montano, 541 U.S. 149, 155–56 (2004))).

18 *See* Clarence & Bessenger, *supra* note 14 (discussing recent border search jurisprudence and attempting to place it in historical context).

19 *See id.*

20 *See id.*

States, require at the least a finding of reasonable suspicion to be constitutional.[21] Non-routine, invasive searches of the person, such as x-rays, strip searches, and cavity searches, have been held to require at least reasonable suspicion,[22] not because the human body receives explicit constitutional protection, but because such searches implicate "dignity and privacy"[23] interests not at issue in regular searches of luggage. Thus, the question of constitutionality may turn on what the criteria are for authorization of a non-routine search.

Though many commentators have chosen to infer the existence of a bright-line rule,[24] the Supreme Court has never chosen to classify property searches as routine and body searches as non-routine. Had the Court intended this, it could easily have said so explicitly in *Flores-Montano*[25] and *Montoya de Hernandez*,[26] instead of leaving open the possibility that some searches of property might be so invasive or intrusive as to require individualized suspicion.[27] It seems logical to conclude that just as not all border searches of the person are considered particularly invasive and thus non-routine, not all searches of property may be considered to be non-invasive and therefore routine.

II. THE BORDER SEARCH DOCTRINE APPLIED TO LAPTOPS AND OTHER ELECTRONIC DEVICES

Thus far, the government has claimed the authority to access the data in electronic devices as it does the objects in a suitcase. The contents of a laptop obviously differ in type and quantity,[28] but there is another, possibly more significant difference between a typical luggage examination and the search of an electronic device—detailed searches of electronic data typically take place after the hard drive has been "mirrored," so that the government retains a perfect copy of

21 *See id.*

22 *See, e.g.*, United States v. Bravo, 295 F.3d 1002, 1006 (9th Cir. 2002).

23 *See* Schmerber v. California, 384 U.S. 757, 769–70 (1966) ("The interests in human dignity and privacy which the Fourth Amendment protects forbid any such intrusions on the mere chance that desired evidence might be obtained.").

24 *See, e.g.*, Sales, *supra* note 3, at 1109–10 (noting that "[t]he Court appears to be drawing a rather bright-line rule" between searches of the body which may in some circumstances require reasonable suspicion, and searches of property, which do not).

25 United States v. Flores-Montano, 541 U.S. 149 (2004).

26 United States v. Montoya de Hernandez, 473 U.S. 531 (1985).

27 *See also Flores-Montano*, 541 U.S. at 152 (rejecting the creation of a complex balancing test to categorize border searches).

28 *See* United States v. Arnold, 523 F.3d 941, 946 (9th Cir. 2008).

all of the information contained therein.[29] Password protection or methods of encryption intended to protect confidential information may offer no security, as travelers have been ordered by Customs agents to enter their passwords before turning over their devices for examination.[30]

Customs is not required to publish records of the circumstances surrounding searches and seizures of laptops and other electronic devices,[31] so much of the data is necessarily anecdotal. Despite this lack of official information, there is no shortage of stories. Kamran Habib, a software engineer and permanent resident of the United States, told the *Washington Post* that his computer and cellular phone were searched three times in one year, and that during one of those searches, an agent went through every phone number and text message stored on his phone.[32] An engineer and U.S. citizen who spoke to the *Post* anonymously was ordered to enter the password to log on to his business computer, over his protests that it belonged to his company and was not his personal property.[33] Bill Hogan, a freelance journalist, had his luggage searched and his laptop seized for nearly two weeks when he returned to the United States from a trip to Germany. He spoke of the particular difficulties facing those in his profession: "It was fortunate that I didn't use [the laptop] for work . . . or I would have had to call up all my sources and tell them that the government had just seized their information."[34]

---

29 *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 540–41 (2005) (explaining "the creation of a perfect 'bitstream' copy or 'image' of the original storage device," which "duplicates every bit and byte on the target drive including all files"); Sales, *supra* note 3, at 1118 ("There is no need to return the bitstream copy to the owner; the owner has the original data in his possession all along, and the government presumably could retain the copy for extended, even infinite, periods of time once the analysis is complete, perhaps perpetually.").

30 *See* David E. Brodsky et al., *At the Border, Your Laptop is Wide-Open*, NAT'L LAW J., July 22, 2008, *available at* http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202423144224) ("[B]order searches, 'from before the adoption of the Fourth Amendment, have been considered to be 'reasonable' by the single fact that the person or item in question had entered into our country from outside.'") (quoting United States v. Ramsey, 431 U.S. 606, 619 (1977)).

31 *Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel: Hearing Before the Subcomm. on the Constitution of the S. Comm. on the Judiciary*, 110th Cong. (2008) [hereinafter *Hearings*] (statement of Susan K. Gurley, Executive Director, Association of Corporate Travel Executives).

32 *See* Ellen Nakashima, *Clarity Sought on Electronics Searches: U.S. Agents Seize Travelers' Devices*, WASH. POST, Feb. 7, 2008, at A1.

33 *Id.*

34 Alex Kingsbury, *Seizing Laptops and Cameras Without Cause: A Controversial Customs Practice Creates a Legal Backlash*, U.S. NEWS & WORLD REP., June 24, 2008,

Individuals attempting to leave the United States are subject to the same suspicionless searches and seizures.[35] Maria Udy, a British citizen living and working in Maryland, was told that unless she handed over her laptop, she would not be permitted to board a flight from Washington, D.C. to London.[36] She was given no reason for the seizure, but instead was asked to provide her log-in information and informed that she would receive her computer within two weeks.[37] While this practice alone is problematic and potentially catastrophic for a businesswoman like Udy (who is employed by a global travel management firm), her story is particularly disturbing because "[m]ore than a year later, Udy [had] received neither her laptop nor an explanation."[38]

Under the Bush administration, Customs and the Department of Homeland Security strongly resisted repeated requests to outline their procedures for the seizure of electronic data, despite Freedom of Information Act requests filed by two non-profit organizations and a written request by Senator Russ Feingold, the Chairman of the Senate Judiciary Subcommittee on the Constitution.[39]

There was cause for optimism as the Obama Administration assumed the helm in early 2009. President Obama could have been speaking directly to outraged civil libertarians—or concerned business travelers—when he stated: "As for our common defense, we reject as false the choice between our safety and our ideals. Our Founding Fathers, faced with perils that we can scarcely imagine, drafted a charter to assure the rule of law and the rights of man."[40] Unfortunately, new hopes have not proven entirely justified thus far.

In August 2009, Homeland Security Secretary Janet Napolitano released new directives on searches of electronic information, for Immigrations and Customs Enforcement and U.S. Customs and Border

---

http://www.usnews.com/articles/news/national/2008/06/24/seizing-laptops-and-cameras-without-cause.html.

35 *See* United States v. Berisha, 925 F.2d 791, 795 (5th Cir. 1991) (extending the border search exception to routine outbound searches). However, in his article defending the current border search policies, Nathan A. Sales notes that "a number of judges and academics have questioned whether the Fourth Amendment permits officials to conduct suspicionless searches of persons or property leaving the country." Sales, *supra* note 3, at 1099 n.31.

36 Nakashima, *supra* note 32.

37 *Id.*

38 *Id.*

39 *See Hearings*, *supra* note 31 (statement of Sen. Russ Feingold, Chairman of Subcomm. on the Constitution, Civil Rights and Property Rights of the S. Comm. on the Judiciary), *available at* http://feingold.senate.gov/statements/08/06/20080625.htm.

40 President Barack Obama, Inaugural Address (Jan. 20, 2008).

Protection.[41] Framed as "guidelines," the directives were perhaps most significant in signaling that the Obama administration is aware of the importance of greater transparency when confronting issues that could have such an enormous effect on so many Americans.[42] They contained general maximums for the length of searches: absent undefined extenuating circumstances, those undertaken by U.S. Customs ought not to take more than five days, and Immigrations and Customs searches ought not to last longer than a month.[43]

Unfortunately, the changes implemented did not go far enough. While travelers may be allowed to be present for at least the initial examination of their laptops (though presumably not for the entire five to thirty days during which a search may occur under "non-extenuating" circumstances), this does not necessarily extend so far as to give them the right to witness the search itself.[44] Permission to sit across the room while Customs officers performed even a cursory examination of the contents of one's laptop or BlackBerry would provide little comfort to an individual carrying confidential or even merely personal information. Elizabeth Goitein, the head of the liberty and national security project at the Brennan Center for Justice, summed up the disappointment of civil liberties groups, stating: "Under the policy begun by Bush and now continued by Obama, the government can open your laptop and read your medical records, financial records, e-mails, work product and personal correspondence—all without any suspicion of illegal activity."[45]

Additionally, information obtained in this way, without any finding of suspicion, can be shared with other government agencies "on a case by case basis, as appropriate."[46] Copies of the information are to

---

41 U.S. Immigration and Customs Enforcement, Dir. 7-6.1, Border Searches of Electronic Devices (Aug. 18, 2009); U.S. Customs and Border Protection, Dir. 3340-049, Border Search of Electronic Devices Containing Information (Aug. 20, 2009).

42 *See* Ellen Nakashima, *Bush's Search Policy for Travelers is Kept*, WASH. POST, Aug. 28, 2009, at A3 (noting that the policy "describes more fully than did the Bush administration the procedures by which travelers' laptops, iPods, cameras and other digital devices can be searched and seized when they cross a U.S. border").

43 U.S. Immigration and Customs Enforcement, Dir. 7-6.1, Border Searches of Electronic Devices (Aug. 18, 2009); U.S. Customs and Border Protection, Dir. 3340-049, Border Search of Electronic Devices Containing Information (Aug. 20, 2009).

44 U.S. Immigration and Customs Enforcement, Dir. 7-6.1, Border Searches of Electronic Devices 3 (Aug. 18, 2009) ("To the extent practicable, border searches should be conducted in the presence of, or with the knowledge of, the traveler."). *See also* Mike M. Ahlers, *Border Rules Revised on Search, Seizure of Electronics, Digital Files*, CNN.COM, Aug. 27, 2009, http://www.cnn.com/2009/US/08/27/borders.computers/index.html.

45 *See* Nakashima, *supra* note 42.

46 U.S. Immigration and Customs Enforcement, Dir. 7-6.1, Border Searches of Electronic Devices 2 (Aug. 18, 2009).

be made for this purpose, and though the directives mandate that copies possessed by Immigration and Customs Enforcement must be destroyed within twenty-one days of the conclusion of the (potentially indefinite) search,[47] no such guarantee exists for additional copies made and shared with other government agencies. Customs may share the copies to receive assistance in the search or for any other purpose, and those agencies may retain the information if it is found to have "national security or intelligence value."[48] There is no indication that a judge will be asked to sign off on this determination or that the individual will be informed of the additional copies that have been disseminated and retained. The vague nature of this authorization is troubling as federal agencies could readily come up with arguments why almost any piece of information might have "value" in the national security or intelligence field.

The policies do mandate that agents document their searches,[49] but they do not provide the traveler with any right to access the documentation in order to find out what information was examined and possibly retained by any federal agency. The traveler is also not provided with notification when and if the search is deemed "completed" and copied information is actually destroyed.

Further, protections for lawyers and others who might be traveling with confidential information are unclear. The directives state essentially that some information may be subject to "special handling" either for policy reasons or by law, but that "a claim of privilege or personal information does not prevent the search of a traveler's information at the border."[50]

A disclaimer that the directives do not create any rights or guarantees that could be invoked by an individual[51] tempers what limited assurance the policies may actually provide to travelers.

---

47 *Id.* at 8.

48 *Id.*

49 U.S. Immigration and Customs Enforcement, Dir. 7-6.1, Border Searches of Electronic Devices (Aug. 18, 2009); U.S. Customs and Border Protection, Dir. 3340-049, Border Search of Electronic Devices Containing Information (Aug. 20, 2009).

50 U.S. Immigration and Customs Enforcement, Dir. 7-6.1, Border Searches of Electronic Devices 9 (Aug. 18, 2009). *See also* Odean L. Volker, *Lawyers, Laptops, and the Border*, 72 TEX. B.J. 640, 643 (2009) (discussing the special dilemma faced by traveling attorneys and noting that, though "both CBP and ICE have recognized the need for special treatment of attorney-client privileged information, neither gives specific guidance on what that special treatment would be or the best practice for raising privilege during a border search").

51 U.S. Immigration and Customs Enforcement, Dir. 7-6.1, Border Searches of Electronic Devices 10 (Aug. 18, 2009).

III. BAD FACTS MAKE BAD LAW—*UNITED STATES V. ARNOLD*

Given that even prominent defenders of the government's application of the border search exception to electronic devices recognize that the practice may be highly offensive to travelers,[52] one would expect to see significant legal challenges brought under the Fourth Amendment. Such challenges might compel courts to order a reconsideration of current practices. Unfortunately, as the saying goes, "bad facts make bad law,"[53] and no "good" factual scenario has turned up in federal court thus far. Individuals seeking to suppress child pornography found on their computers have brought every serious courtroom challenge to the constitutionality of the border search exception as applied to electronic devices,[54] and, not surprisingly, they have proven to be unsympathetic plaintiffs.[55]

In the most recent high-profile case, *United States v. Arnold*, the U.S. District Court for the Central District of California held that applying the border search doctrine to laptop computers was excessively intrusive and violated the Fourth Amendment.[56] The court granted a motion to suppress child pornography found on the defendant Arnold's laptop during a suspicionless border search because "[w]hile not physically intrusive as in the case of a strip or body cavity search, the search of one's private and valuable personal information stored on a hard drive or other electronic storage device can be just as much, if not more, of an intrusion into the dignity and privacy interests of a person."[57] The court held that border searches of electronic storage devices must be based on reasonable suspicion at a minimum.[58]

---

52 *See, e.g.*, Sales, *supra* note 3.

53 *See, e.g.*, Haig v. Agee, 453 U.S. 280, 319 (1981) (Brennan, J., dissenting). *See also* United States v. Montoya de Hernandez, 473 U.S. 531, 548 (1985) (Brennan, J., dissenting) ("It is a fair summary of history to say that the safeguards of liberty have frequently been forged in controversies involving not very nice people." (quoting United States v. Rabinowitz, 339 U.S. 56, 69 (1950) (Frankfurter, J., dissenting))).

54 *See, e.g.*, United States v. Arnold, 533 F.3d 1003 (9th Cir. 2008); United States v. Hilliard, 289 F. App'x 239 (9th Cir. 2008); United States v. Romm, 455 F.3d 990 (9th Cir. 2006); United States v. Ickes, 393 F.3d 501 (4th Cir. 2005).

55 *See* Matthew R. Hall, *Border Fiction: Does an Analogy to Immigration Law Alleviate Fourth Amendment Anxiety?*, 78 MISS. L. J. 363, 378 (2008) (claiming that "if the cases most actively litigated arise out of those 'hits' rather than out of the 'misses,' [where a search was unjustified], a danger arises. The search program superficially appears successful after the fact of a positive result—it appears justified because it succeeded").

56 454 F. Supp. 2d 999 (C.D. Cal. 2006).

57 *Id.* at 1000.

58 *Id.* at 1001.

On April 21, 2008, the Ninth Circuit reversed this holding, refusing to distinguish between an electronic device and any other container brought into the country.[59] The Court of Appeals held that the lower court erred in applying an intrusiveness analysis to the search of Arnold's laptop, stating that the Supreme Court's opinion in *Flores-Montano* precluded the use of that standard for property searches.[60] The court rejected Arnold's attempt to analogize the privacy expectations for a laptop to those for the home.[61] The opinion stated that case law did not support a finding that a search could be considered especially offensive due to the storage capacity of the object being searched,[62] but acknowledged that "the Supreme Court has left open the question of whether, and under what circumstances, a border search might be deemed unreasonable because of the particularly offensive manner in which it is carried out."[63]

This ruling was a significant setback for groups concerned with the civil liberties and privacy interests of international travelers, who had applauded the district court decision for distinguishing border searches of laptops from traditional searches of luggage or other belongings.[64]

IV. INHERENT DIFFERENCES IN SEARCH OR SEIZURE OF INFORMATION STORED ON ELECTRONIC DEVICES

People today are mobile to a degree that the Framers could hardly have imagined. Their computers frequently function as mobile offices, contain more than any file cabinet ever could and retain every file or piece of data ever accessed. Judge Pregerson, who authored the district court opinion in *Arnold*, wrote that laptops and similar devices "function as an extension of our own memory."[65] If the Fourth Amendment is meant to protect the individual's reasonable expecta-

59 533 F.3d 1003 (9th Cir. 2008), *cert. denied*, 129 S. Ct. 1312 (2009).

60 *Id.*

61 *Id.* at 1008.

62 *Id.* at 1009–10.

63 *Id.* at 1008 (internal quotation marks omitted).

64 *See* Electronic Frontier Foundation, Travel Screening, http://www.eff.org/issues/travel-screening (last visited Feb. 16, 2010) (claiming that "the ongoing searches of laptops, cell phones, and other electronic devices at America's borders are unconstitutionally invasive"); Association of Corporate Travel Executives, Traveler Security and Data Privacy, http://www.acte.org/content/laptop_seizures (last visited Feb. 16, 2010) (noting that travelers have had to react to requirements that can prove an impediment to the conduct of business).

65 United States v. Arnold, 454 F. Supp. 2d 999, 1000 (C.D. Cal. 2006), *rev'd*, 533 F.3d 1003 (9th Cir. 2008).

tion of privacy,[66] it is logical to consider how innovations in technology might alter the circumstances in which an individual's privacy interest merits particular protection. This in turn requires consideration of how new technologies may have altered the individual's expectation of privacy.[67]

In the Fourth Amendment context, federal courts have repeatedly found that individuals have a reasonable expectation of privacy in the contents of their own computers.[68] In fact, owners have a reasonable expectation of privacy in the contents of any closed container,[69] including the data stored inside electronic devices.[70] Outside of the border-search context, extensive protections are available to ensure the security of privileged or proprietary information: attorney-client protections are among the highest privileges granted under law, and the crucial confidentiality of business information such as trade secrets, journalistic sources, potential merger agreements, and reports on internal investigations can be all but guaranteed by contractual arrangements. To establish an end-run around these considerations, otherwise sanctioned by United States law, merely because a law-abiding citizen chooses to cross the border, injects an inappropriate and potentially unlimited amount of uncertainty into the normal course of business for the individual and his or her employer.

The search and seizure of data on a laptop computer is simply too intrusive to be considered a "routine" border search and, as such, likened to the physical examination of an individual's luggage for drugs or stolen property. The Supreme Court has stated that "physical entry of the home is the chief evil against which the wording of the

66 *See, e.g.*, Sara M. Smyth, *Searches of Computers and Computer Data at the United States Border: The Need for a New Framework Following* United States v. Arnold, U. ILL J.L. TECH. & POL'Y 69, 95 (2009) ("The question of whether an individual has a reasonable expectation of privacy is the *sine qua non* of a Fourth Amendment search.").

67 Even experienced travelers are unaware of the degree to which their devices are subject to search. Press Release, Ass'n of Corporate Travel Executives, *supra* note 3.

68 *See, e.g.*, United States v. Buckner, 473 F.3d 551, 554 n.2 (4th Cir. 2007) (recognizing a reasonable expectation of privacy in password-protected computer files); United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) ("Individuals generally possess a reasonable expectation of privacy in their home computers.").

69 United States v. Ross, 456 U.S. 798, 822–23 (1982).

70 *See* United States v. Barth, 26 F. Supp. 2d 929, 936 (W.D. Tex. 1998) ("[T]he Fourth Amendment protection of closed computer files and hard drives is similar to the protection it affords a person's closed containers . . . . [T]he owner's expectation of privacy relates to the contents of that container rather than the container itself.") (citation omitted); United States v. Chan, 830 F. Supp. 531, 534 (N.D. Cal. 1993) (finding that an individual's privacy interest in a pager and its data is analogous to that in any other closed container).

Fourth Amendment is directed,"[71] but also that, "the Fourth Amendment protects people, not places"[72]—and the protections bestowed should not be entirely obliterated simply because a person opts to travel in or out of the United States. In every search and seizure of electronic information, there is enormous potential for a violation of the owner's expectation of privacy, such that the reasonable suspicion requirement should be extended to in-depth searches of laptops and other electronic devices at the border.[73]

Contrary to the claims of the Department of Homeland Security, the devices are conceptually very different from a suitcase. Some commentators have presented persuasive arguments that due to the personal nature of the information therein and the privacy interest of the owner, examinations of laptop computers ought to be analogized to searches and seizures taking place in the home or the office.

In a recent article, commentator Rasha Alzahabi discusses one compelling reason to regard searches of electronic data differently than other items brought across the border: the contents of electronic devices are intangible.[74] As justifications of the border search exception to the Fourth Amendment's warrant requirement "are usually framed in terms of 'who and what may enter the country,' these justifications do not apply to suspicionless laptop border searches. The information saved on a laptop can be transported into our country electronically, regardless of whether the traveler or the laptop crosses the border."[75]

Alzahabi also expresses doubt about the constitutionality of a warrantless search that is intended to find general evidence of illegal activity, whether in the form of terrorist attack plans or caches of child pornography.[76] She cites *Colorado v. Bertine*, a case considering the

---

71 Payton v. New York, 445 U.S. 573, 585 (1980) (quoting United States v. U.S. Dist. Court, 407 U.S. 297, 313 (1972)).

72 Katz v. United States, 389 U.S. 347, 351 (1967).

73 *See, e.g.*, Smyth, *supra* note 66, at 95 ("Given their unique ability to reveal vast amounts of highly personal information, in which an individual has a reasonable expectation of privacy, these searches must be viewed as nonroutine and preceded by reasonable suspicion.").

74 Rasha Alzahabi, *Should You Leave Your Laptop at Home When Traveling Abroad?: The Fourth Amendment and Border Searches of Laptop Computers*, 41 IND. L. REV. 161 (2008).

75 *Id.* at 175 (quoting United States v. Ramsey, 431 U.S. 606, 620 (1977)). *See also* Erwin Chemerinsky & Karen M. Blum, *Fourth Amendment Stops, Arrests and Searches in the Context of Qualified Immunity*, 25 TOURO L. REV. 781, 821 (2009) (noting that "the law enforcement justification that has always been stressed with regard to the border are illegal immigration of individuals, contraband, weapons—that seems so unlikely when you turn on a laptop and see the files").

76 Alzahabi, *supra* note 74, at 177.

constitutionality of examining closed containers during routine inventory searches of automobiles.[77] There, the Supreme Court specified that searches made "solely for the purpose of investigating criminal conduct" must meet warrant (and attendant probable cause) requirements as mandated by the Fourth Amendment.[78] "Thus," she argues, warrantless and "intrusive border searches may not be conducted solely for the purpose of catching criminals or terrorists; rather, they must be consistent with the traditional rationales justifying the border search—the prevention of the entry of illegal aliens and contraband into our country."[79] Although Alzahabi does not explore this issue in depth, focusing instead on the intrusiveness of laptop searches,[80] the "purpose" distinction is important: searching through someone's luggage in the typical manner clearly serves the "traditional rationales" of the border search—it will be revealed if he or she is attempting to conceal items or people prohibited in the United States. To require particularized suspicion before any search would render every ordinary, random luggage inspection constitutionally questionable. The border search exception when applied to electronic data seems to target different types of crimes. Further, if searches in the name of looking into general "criminal conduct" are impermissible without a warrant, it seems illogical that searches of laptop computers *leaving* the country can be constitutionally conducted without any suspicion or finding of probable cause.[81] A more appropriate balance can and should be struck between the competing interests of privacy and security.

Previous legal commentary on the subject has tended to focus on the rights of individuals whose electronic devices may contain illicit information. While it is essential to protect the rights of criminal defendants, it is equally important to consider the impact of these search policies on individuals who are not engaging in illegal behavior—after all, they are less likely to challenge the procedures but may be impacted just as significantly.[82]

---

77 479 U.S. 367 (1987).

78 *Id.* at 371.

79 Alzahabi, *supra* note 74, at 176. *See also* BRUCE A. NEWMAN, AGAINST THAT "POWERFUL ENGINE OF DESPOTISM": THE FOURTH AMENDMENT AND GENERAL WARRANTS AT THE FOUNDING AND TODAY ix (2007) (analyzing the limitations placed on searches aimed at criminal activity).

80 Alzahabi, *supra* note 74, at 178.

81 *Id.* at 176–77 (discussing various reasons in favor of requiring suspicion for laptop border searches).

82 *See* Hall, *supra* note 55, at 378 (noting that border searches "affect an enormous number of individuals for each case that nets the government criminal conduct").

V. SPECIAL CONCERNS OF PRIVILEGE AND CONFIDENTIALITY

The federal courts have previously justified the border search doctrine by finding that the United States "has an overriding interest in securing the safety of its citizens" in preventing the entry of contraband, and that "greater interest on the side of the government at the border is coupled with a lesser interest on the side of the potential entrant."[83] While this may be the case when the "potential entrant" attempts to bring in child pornography, the law-abiding attorney or business traveler maintains a critical interest in preserving the security of the information on his laptop or other electronic device.

In *United States v. Arnold*, the Ninth Circuit noted that the Supreme Court has left open the possibility of a reasonable suspicion requirement for some types of border searches of property—for example, searches that are especially damaging.[84] The court noted that the defendant never raised the issue of "exceptional damage to property" but that defendant did claim that the procedures inflicted upon him were "particularly offensive," and it rejected the latter argument.[85] A traveler whose information could be considered valuable property, wholly or in part because of its confidentiality, should have a much stronger claim that a search was exceptionally damaging or particularly offensive if it resulted in the seizure, reproduction, or loss of confidentiality of his information.

Issues of confidentiality in other contexts reaffirm the argument that as searches of computers present such a great danger of infringing on privacy rights, the application of the traditional border search exception provides inadequate protection.[86] Attorney-client communications are privileged in the United States, and federal courts have held that the constitutional right to effective legal representation and the privilege against self-incrimination justify this protection.[87] The

---

83 United States v. Ickes, 393 F.3d 501, 506 (4th Cir. 2005).

84 523 F.3d 941, 946 (9th Cir. 2008) (citing United States v. Flores-Montano, 541 U.S. 149, 155–56 (2004)).

85 *Id.* at 946–47 ("Whatever 'particularly offensive manner' might mean, this search certainly does not meet that test. Arnold has failed to distinguish how the search of his laptop and its electronic contents is logically any different from the suspicionless border searches of travelers' luggage that the Supreme Court and we have allowed.").

86 Indeed, at least one commentator has argued persuasively that a whole new standard ought to be developed. *See* Smyth, *supra* note 66, at 84 ("The risk is that if we confine ourselves to using traditional analogies, we cannot fully articulate what is fundamentally different about our privacy interests in information technology.").

87 *See* JONATHAN AUBURN, LEGAL PROFESSIONAL PRIVILEGE: LAW AND THEORY 28 (2000) (discussing the protection of attorney-client communications and attorney-work product in

purpose of the attorney-client privilege, as stated by then-Justice Rehnquist, is "to encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice."[88] Confidentiality must be guaranteed to prevent chilling of communications between attorney and client, and to ensure that lawyers can effectively perform their function in society.[89] In this increasingly digitized age, attorneys frequently carry confidential information on their computers and personal digital assistants such as BlackBerrys. The attorney's ability and duty to keep information confidential is certainly compromised when Customs agents can copy all of the data on an electronic storage device and the attorney is not given an explicit opportunity to protect the confidentiality of specific files or even to ensure that all copies have been securely destroyed. As discussed briefly above, the manner in which an attorney might prevent such invasion is as yet undefined in the policies released by the Department of Homeland Security.[90]

The duty to keep information confidential is not unique to attorneys. Physicians and psychologists carry patient records. Business travelers may carry sensitive information detailing, for example, trade secrets or plans for taking a company public that they are contractually obligated to keep private. While the legal and ethical violations in the above examples would not rise to the level of constitutional claims, they certainly provide support for the argument that the expectation of privacy in such information is sufficiently reasonable to require some level of suspicion before it is seized, copied, or searched.[91]

The border-search exception as applied to electronic storage devices has never been subjected to a serious challenge by an individual who was not carrying illicit data, but such a scenario is certainly plausible. Consider an American investment company that handles the portfolios of major foreign companies or even foreign governments.

---

the United States as justified instrumentally because of concerns about effective legal counsel and representation).

88 Upjohn Co. v. United States, 449 U.S. 383, 389 (1981).

89 *See* AUBURN, *supra* note 87, at 66 ("The argument often raised for absolute confidentiality is that without it people would be reluctant to speak openly and honestly with their lawyers . . . .").

90 *See supra* notes 41–51and accompanying text.

91 *See* Nakashima, *supra* note 32 (quoting Georgetown law professor David D. Cole: "What a laptop records is as personal as a diary but much more extensive. It records every Web site you have searched. Every e-mail you have sent. It's as if you're crossing the border with your home in your suitcase.").

The investment information would be sensitive and confidential but perfectly legal to possess. If a representative of the company travels in and out of the United States to do business and has stored this information on his computer (even if password protected), the United States government may "mirror" the individual's hard drive, creating and retaining a perfect copy, or seize the original computer itself. This could be enormously costly or even paralyzing for a businessperson or another individual carrying critical, time-sensitive information. The traveler has no way of knowing what information was examined, or if perhaps the mirrored hard drive has been lost or further reproduced and disseminated somewhere in an enormous governmental bureaucratic maze.

In the event that such a search does take place, the investment company may have an obligation to notify its foreign client that the information is in the possession of the United States government.[92] It seems likely that, faced with such a possibility, the client may elect to do business only with local investment firms in the future.

This is not an argument for a constitutional guarantee for United States businesspeople to work overseas, however the potential for such a situation indicates that the reasonable expectation of privacy in the contents of computers belonging to individuals and corporations should be taken into account in the creation of border search policies. If the same businessman was carrying a briefcase full of documents, the Customs agent would likely sift through it briefly—it is fantastical to imagine the agent, with no suspicion whatsoever, photocopying every item in the briefcase (and passing on additional copies to other government agencies) before returning the originals to their owner.[93] It is even less likely that the briefcase would actually be seized from its owner for some period of time.

The differences discussed above demonstrate that Judge Pregerson was correct to conclude that "opening and viewing confidential computer files implicates dignity and privacy interests"[94] and that "the information contained in a laptop and in electronic storage devices

---

92 *See* Smyth, *supra* note 66, at 85 ("[C]ustoms officials can now copy and analyze confidential business files that may contain trade secrets or personal information about a company's clients. If the computer happens to belong to an attorney, the government can seize and copy privileged information. This could result in a breach of confidentiality and may give rise to an obligation to notify clients of a security breach.").

93 Even if this did occur, such copies could be more easily secured and would not take nearly as long to examine for evidence of illegality. Electronic data has infinitely more potential to be lost, stolen, corrupted, or otherwise compromised.

94 United States v. Arnold, 454 F. Supp. 2d 999, 1003 (C.D. Cal. 2006), *rev'd*, 523 F.3d 941 (9th Cir. 2008).

renders a search of their contents substantially more intrusive than a search of the contents of a lunchbox or other tangible object."[95] The Electronic Frontier Foundation and Association of Corporate Travel Executives, in their joint brief to the Ninth Circuit in *Arnold*, explained the objective reasonableness of a strong expectation of privacy in one's laptop computer: the information contained on a citizen's laptop computer "is unique in its private nature, in its nearly limitless volume, in its pervasive role in our society, and in its capacity to be quickly copied, saved, and searched."[96] The nature of items in existence when the border search doctrine was established simply cannot be analogized to laptops and the like in any way that would justify suspicionless searches of the latter.

VI. ADDRESSING COUNTERARGUMENTS

Supporters of the government's claim of full search authority argue that national security concerns outweigh any liberty or privacy infringement that might come about as a result of the policies.[97] Kelly Gilmore cautions against "[e]stablishing immunity for digital information at the border,"[98] envisioning dire results for both the War on Terror[99]—she notes the use of computers in planning the attack on the World Trade Center in 1993[100] as well as a raid on a Pakistani home that uncovered computers containing data "indicating al Qaeda's resolve to commit more attacks on United States soil"[101]—and the

95 *Id.*

96 Brief for Ass'n of Corporate Travel Executives and Electronic Frontier Foundation as Amici Curiae Supporting Defendant-Appellee at 7, United States v. Arnold, 533 F.3d 1003 (9th Cir. 2008) (No. 06-50581). Even the Ninth Circuit, which overturned the District Court's requirement of reasonable suspicion for laptop searches at the border, recently acknowledged that individuals "undoubtedly have a high expectation of privacy in the files stored on their personal computers." United States v. Adjani, 452 F.3d 1140, 1146 (9th Cir. 2006).

97 *See, e.g.*, Kelly Gilmore, *Preserving the Border Search Doctrine in a Digital World: Reproducing Electronic Evidence at the Border*, 72 BROOK. L. REV. 759, 786 (2007) ("The compelling security interests in the border context far outweigh the information privacy interests a traveler may reasonably expect to have, especially in the context of personal objects. Privacy expectations for the information contained in electronic devices are simply unreasonable and the consequences of such immunity would be enormous.") (citations omitted).

98 *Id.*

99 *See id.* at 787–88 ("As the rest of the world has turned to laptops and wireless communication devices for the storage of personal information, it appears terrorists have as well.").

100 *Id.* (citing Michael A. Vatis, *Cyber Attacks: Protecting America's Security Against Digital Threats*, *in* COUNTERING TERRORISM 219, 229 (Arnold M. Howitt & Robyn L. Pangi eds., 2003)).

101 *Id.* at 788 (citing Bill Powell, *Al-Qaeda in America: The Terror Plot*, TIME, Aug. 16, 2004, at 28).

War on Drugs, in that it would prevent the uncovering of digital evidence of "trafficking conspiracies."[102]

Gilmore also points to the record-keeping procedures maintained by Customs, referring to Justice Breyer's concurrence in *Flores-Montano*[103] for support of the proposition that the keeping of records offers adequate protection to those who experience the seizure of their data.[104] But the retention of "administrative" records by the federal government is of little use if individuals cannot get to them—how are they to know why their information was seized or who has seen their data?

Child pornography and terrorist schematics should certainly be prevented from entering the United States. Anecdotes and court challenges described herein show that a few border searches have lead to the detection of child pornography. There is no disputing that the government has a compelling interest in the control and prevention of such activity, but a reasonable suspicion standard would still allow for the search of the computers of likely offenders.[105]

On the other hand, it is nearly incredible to imagine the frequent unmasking of terrorist plots on an individual's computer during a suspicionless border search. A traveler possessing truly dangerous data will almost certainly encrypt it heavily and nearly invisibly, or transmit it over the Internet rather than attempt to bring it into the United States on a hard drive.[106] Using vague threats to justify the suspicionless, unchecked search and seizure of information from an unlimited number of travelers, while providing them no method of recourse in order to track their data and no enforceable guarantees of its security and confidentiality, infringes the liberty of millions of individuals in the name of insufficient and unfocused protection.[107]

---

102 *Id.* at 788–89 (citing United States v. Fortna, 796 F.2d 724, 738 (5th Cir. 1986)).

103 United States v. Flores-Montano, 541 U.S. 149, 156 (2004) (Breyer, J., concurring) ("Customs keeps track of the border searches its agents conduct . . . . This administrative process should help minimize concerns that . . . searches might be undertaken in an abusive manner.").

104 Gilmore, *supra* note 97, at 794–95.

105 *See* United States v. Montoya de Hernandez, 473 U.S. 531, 541 (1985) ("The 'reasonable suspicion' standard has been applied in a number of contexts and effects a needed balance between private and public interests when law enforcement officials must make a limited intrusion on less than probable cause.").

106 *See* Thomas Claburn, *Business, Cyber Liberties Groups Fight Laptop Searches*, INFORMATIONWEEK, June 13, 2008, http://www.informationweek.com/news/security/client/showArticle.jhtml?articleID=208403992 ("The fact that such content can travel more or less unhindered over the Internet can be seen either as ironic or as a sign that the Internet will eventually be subjected to the same broad scrutiny (if it isn't already).").

107 *See* Mitchell Zimmerman, Fenwick & West LLP, Privacy Alert: Gov't Rummaging Through Your Laptop's Contents? No Problem if You're Re-Entering USA, Says Ninth

Law professor and former Department of Justice and Department of Homeland Security official Nathan A. Sales provides perhaps the most persuasive defense of the government's application of the border search exception to laptops and other electronic storage devices in an article entitled *Run For the Border: Laptop Searches and the Fourth Amendment*.[108] He uses the history of the border search doctrine and the principle of "technological neutrality"[109]—the notion that the manner in which information is stored and carried by a traveler should not be a factor in the degree of protection it receives—to argue that suspicionless searches of laptops are constitutional.

In arguing that the border search doctrine is constitutional as presently applied to electronic storage devices, Sales analogizes to international mail.[110] He discusses the Supreme Court's opinion in *United States v. Ramsey*, which held that it was constitutional for Customs officials to search incoming international mail for contraband.[111] The Court emphasized that it should not matter if an envelope or package enters the country in the hands of a traveler (thus subject to suspicionless search under the border search doctrine) or by mail.[112] Therefore, Sales argues that "[t]he mere fact of computerization shouldn't make a difference"[113] but this may be an inapposite analogy—after all, if data is sent into the country electronically it is not subject to suspicionless search and indefinite seizure. When it comes to privacy protections for documents "sent" into the United States, computerization makes all the difference.

Further, laptop searches themselves are not technologically neutral. It takes little time for a border officer to rifle through a suitcase

---

Circuit (2008), http://www.fenwick.com/docstore/Publications/Litigation/Privacy_Alert_04-30-08.pdf ("[W]hile Customs asserts that its officers 'are trained to protect confidential information,' it is difficult to know what this means in practice."). Zimmerman envisions a number of potentially problematic scenarios implicating business plans, trade secrets, and legal information and goes on to note, "[o]n the other hand, if you actually are an al Qaeda terrorist, you will not likely find yourself seriously inconvenienced by these practices. Insofar as a terrorist's plans might require written materials, he can simply email them to himself and travel without a computer, purchasing a new one after arrival in the United States." *Id.* *But see* Sales, *supra* note 3, at 1097–98 ("Moderately sophisticated terrorists and child predators could accomplish the same thing by uploading materials to a private server . . . . Yet the fact that terrorists and others might use a number of techniques to commit their crimes does not diminish the magnitude of the government's interest in inhibiting this particular technique.").

108 Sales, *supra* note 3.

109 *Id.* at 1093.

110 *Id.* at 1109.

111 *Id.* (citing United States v. Ramsey, 431 U.S. 606 (1977)).

112 *Ramsey*, 431 U.S. at 620.

113 Sales, *supra* note 3, at 1116 (footnote omitted).

to make sure that no contraband is being smuggled in, or to flip through a stack of photos to check for child pornography. On the other hand, due to their enormous storage capacity, examinations of computers can take days, and thus are often performed with "mirrored" hard drives. As Professor Smyth notes, deleted information is also readily recoverable in the search.[114] If a suitcase search turned up everything that had ever been carried inside of it, even a cursory examination would be rendered much more invasive.

Professor Sales demonstrates awareness that privacy and free expression concerns are implicated whenever a border search of a laptop computer or other storage device takes place.[115] He mentions the special plight of the journalist, the attorney, or the business traveler, noting that current policies mean that "[p]eople who cannot realistically minimize their expressive activities, such as journalists, opinion leaders, and activists, might cope with border searches by minimizing their overseas travel," while "[p]eople who cannot realistically minimize their overseas travel, such as global businessmen, might cope with border searches by minimizing their expressive activities. Either way, there is a risk that core constitutional values will be chilled."[116]

Ultimately, Sales concludes that the differences between a laptop and conventional luggage "do not justify a blanket 'laptop exception' to the border search doctrine."[117] This is undoubtedly true; however, there is no reason to conclude that because a blanket exemption would be unjustified, no protection is in order. Instead, the courts should recognize that while "the expectation of privacy [is] less at the border than in the interior,"[118] it still exists, and a reasonable suspicion standard is an appropriate middle ground.[119]

Despite his overarching conclusion that the Fourth Amendment itself offers "relatively weak constitutional protections" for these significant issues,[120] Sales does allow that a number of potentially beneficial regulations could be implemented. His article suggests that the Department of Homeland Security provide as much information as

---

114 Smyth, *supra* note 66, at 94.

115 Sales, *supra* note 3, at 1092 ("The most intimate details of a person's life—e-mails to friends and colleagues, family photographs, financial records, and so on—are paraded in front of the officers at the customs checkpoint.").

116 *Id.* at 1101.

117 *Id.* at 1093–94.

118 United States v. Montoya de Hernandez, 473 U.S. 531, 539 (1985).

119 Some scholars argue for much stronger protections. For a few examples, *see* Sales, *supra* note 3, at 1106 n.81.

120 *Id.* at 1094.

possible to the public about its search and seizure practices,[121] noting that increasing public knowledge about these procedures (as well as formalizing standards for choosing who to search) will help prevent abuses.[122] He calls for guidelines in the length of time a search may take.[123] Most intriguing, he analogizes to minimization requirements in the domestic wire-tapping context and similar rules in the Foreign Intelligence Surveillance Act to suggest limits on the scope of a search when no criminal activity is initially uncovered.[124]

A routine inspection of a suitcase is drastically different from the copying or seizure of the hard drive of a computer or PDA. Customs agents acting without any suspicion should be able to open laptop computers and even ask their owners to turn them on, to be sure that they are what they seem to be and that they belong to their carriers. It is an enormous conceptual leap from that idea to the current state of the law—with no particular reason for concern, a Customs agent can order an individual entering or leaving the United States to enter his or her password into a computer and to leave behind the device, or one or more mirrored copies of its contents, without any recourse.[125]

VII. ESTABLISHING A BETTER BALANCE

The current government border search policies pose a threat to Fourth Amendment guarantees when applied to laptops and similar devices. Either the legislature or the courts should step in and mandate protections for travelers crossing the border. The legislature is perhaps better suited to implement such protections,[126] and individu-

---

121 *Id.* at 1128.

122 *Id.* at 1128–30. This raises the intriguing and disturbing hypothetical that a truly well-informed public would then have no subjective expectation of privacy, which erodes any Fourth Amendment claim in this context but does nothing to protect civil liberties.

123 *See id.* at 1130 ("Unfortunately, the [DHS] Policy Statement does not do much in this regard. It merely recites the boilerplate goal that searches of laptops should be completed within 'a reasonable period of time.'" (footnote omitted)).

124 *Id.* at 1131.

125 *See* Steve Seidenberg, *9th Circuit: Laptops May Be Subject to Customs Inspections After Overseas Trips*, 5 A.B.A. J. EREPORT, Sept. 15, 2006, at 37 (quoting Shaun Martin, a law professor at the University of San Diego: "It is one thing to turn on your computer in the airport to make sure it is not a bomb. It is another thing for customs officials to turn on your computer and to read everything you ever wrote and to look at everything you ever downloaded.").

126 *See* Posting of Jennifer Granick to Deeplinks, http://www.eff.org/deeplinks/2008/05/protecting-yourself-suspicionless-searches-while-t (May 1, 2008) (suggesting that individuals contact their congressional representatives to express disagreement with the current governmental policies).

als concerned with their civil liberties should contact their congressional representatives to continue to raise the profile of this issue.[127]

The Supreme Court or Congress ought to establish definitively that reasonable suspicion of wrongdoing is necessary to legitimize searches or duplication of electronic information at the border, and Customs agents should be required to make the record of the search and the basis for finding particularized suspicion available to the affected individual.

An important first step is acknowledgement that it is possible to perform both a routine and a non-routine search of a laptop computer. A routine search might include a request for the owner to turn on the computer and perhaps even an examination of recently-accessed or created files, strictly limited in time and scope and always in the presence of the owner. Performing such a search in front of the owner would alleviate some concerns regarding the confidentiality of certain information.

Further, when a hard drive is "mirrored," a warrant should be required before any information from it is decrypted or passed on to another federal agency.[128] Because a reproduction has been made and the individual subject to search is not being deprived of the use of his or her property, there is less argument that exigent circumstances prevent the typical resort to judicial oversight. An impartial magistrate could also determine whether information has sufficient "value" to "national security or intelligence" to merit being passed on to other agencies. This is particularly important as, according to the Department of Homeland Security, the agencies may retain any information based on their own "independent legal authority"—although they would not have had the authority to seize it in the first place.

---

127 Not all legislators have been silent. Senator Russ Feingold introduced the Travelers' Privacy Protection Act in the Senate, which would require reasonable suspicion before laptop searches and would limit seizures of electronic devices without probable cause to twenty-four hours. Travelers' Privacy Protection Act of 2008, S. 3612, 110th Cong. (2008). Loretta Sanchez introduced the Border Security Search Accountability Act of 2008 in the House, which calls for the establishment of a procedure to notify individuals if their data has been copied. Border Security Search Accountability Act of 2008, H.R. 6869, 110th Cong. (2008). Both bills died shortly after introduction and were never put to a vote. Govtrack.us, S. 3612, Travelers' Privacy Protection Act of 2008, http://www.govtrack.us/congress/bill.xpd?bill=s110-3612; Govtrack.us, H.R. 6869, Border Security Accountability Act of 2009, http://www.govtrack.us/congress/bill.xpd?bill=h110-6869.

128 Even Professor Sales, who defends the government policies, notes that with the practice of mirroring hard drives, "[l]aptop searches . . . raise the specter of officers retaining sensitive data from an entirely innocent passenger's computer for months, maybe even years." Sales, *supra* note 3, at 1124.

Strict guidelines should be established to ensure that travelers have a way of knowing what information has been copied, and to mandate notification when the information is destroyed after a determination that it does not contain anything illicit.

In the meantime, companies and individuals that deal with potentially privileged, confidential, or time-sensitive information should be aware that anything stored on their PDAs, BlackBerrys, or computer hard drives can be examined, seized, and copied by the United States government during a border search. Until a policy that better balances liberty and privacy concerns with those of national security is implemented, the safest solution is to leave electronic devices behind when leaving the United States.

It is not the potential for enormous storage capacity, but rather the nature of what is stored and the invasion necessary to perform the search, that distinguishes the search and seizure of information on electronic storage devices from traditional border searches, and renders the former potentially "particularly offensive" and "exceptionally damaging."[129]

The adoption of a reasonable suspicion standard, as well as the specific protections discussed herein, would better protect both the common defense and the rights of the individual. When faced with the next constitutional challenge, one hopes that the courts will cease to allow national security justifications to erode protection of civil liberties at the border.

---

129 *See* United States v. Arnold, 523 F.3d 941, 947 (9th Cir. 2008) ("[C]ase law does not support a finding that a search which occurs in an otherwise ordinary manner, is 'particularly offensive' simply due to the storage capacity of the object being searched.").